splunk>

CASE STUDY

Splunk® at Nevada Department of Transportation

State Agency Turns to Splunk to Bolster Security & Operational Efficiencies

"Whenever there's a problem, we immediately go to Splunk for optics and intelligence. Splunk has empowered us to plug security gaps, improve efficiencies and save taxpayer money. We're limited only by our imaginations as to all the ways we can leverage the platform."

Information Security Officer
Nevada Department of Transportation

OVERVIEW

INDUSTRY
- State government

SPLUNK USE CASES
- Security
- Compliance
- Operational intelligence
- IT/Ops
- Application management

BUSINESS IMPACT
- Optimized security posture
- Cost savings and improved operational efficiencies due to identifying misconfigurations
- Rapid issue resolution and immediate operational visibility
- Improved public safety
- More efficient resource management
- Enhanced productivity

DATA SOURCES
- Log events from traffic control systems
- Log events from servers, switches, routers & firewalls
- Log events from FTP servers
- Logs from network printers
- MS Active Directory logs

PRODUCT
- Splunk Enterprise

The Agency

Since its creation in 1917, the Nevada Department of Transportation (NDOT), a division of Nevada's state government, has been enhancing public safety and commerce by planning, constructing, operating and maintaining the state's highways. Today, the department is responsible for the 5,400 miles of highway and over 1,000 bridges that comprise Nevada's highway system. NDOT also oversees the state's 511 system, which enables citizens to determine road conditions and delays caused by construction or natural events like rock slides, and a statewide video camera network that allows motorists to view traffic levels prior to travelling. The department is based in Carson City and has approximately 2,000 employees throughout the state.

Challenges

NDOT's information security officer sought better reporting from the department's Internet content filtering solution to document web activity. She was concerned that too many employees believed that hackers are only motivated to steal information that they can monetize and, therefore, NDOT was not at risk. The ISO understood that hackers from rogue nations and elsewhere seek to cause economic and social disruptions, which makes NDOT, responsible for transportation infrastructure, a target. She had to identify the agency's security vulnerabilities and document attempted hacks into its network. However, NDOT's manual processes for system log reviews were tedious, unreliable and often tardy. To gain visibility into network traffic, the ISO needed to systematically collect the logs from various hosts as well as those from web servers.

Enter Splunk

The department's technology staff knew of Splunk's reputation within the IT security community and the platform's ability to aggregate and display unstructured data from sources across a networked infrastructure. The team initially downloaded Splunk Enterprise for a trial and the ISO used the Splunk dashboard editor to build two dashboards to graphically present and manage logs for diagnosis and troubleshooting. One captures logs from the department's web and FTP servers to track security events. The other collects data from servers, switches, routers and firewalls throughout the network to inform staff of events like errors, time-outs, crashes and alerts.

Once NDOT began sending log event data from across their infrastructure into Splunk, they immediately gained operational visibility into security and IT/Ops issues that had previously taken numerous man-hours to resolve. According to the ISO, "Splunk software automates the laborious process of sifting through logs and other machine-generated data, which saves time and trouble identifying the source of problems. Splunk gives us both holistic and granular views of our IT environment, enabling us to do root-cause analyses very quickly."

Breakthroughs

Even prior to the full deployment of Splunk at NDOT, the security team soon found that a variety of networked devices were misconfigured, which potentially

compromised security and performance. For example, on the morning a firewall was installed at a remote location, NDOT discovered via Splunk that someone overseas was attempting to use the device to access the network. Thanks to Splunk, the firewall was correctly reconfigured that afternoon to deny such outside connections, plugging what could have been a costly security hole for NDOT. This helped to bolster the agency's defenses and enabled the ISO to verify the many attempts by hackers to penetrate NDOT's network.

Once Splunk software was fully implemented at NDOT, it quickly proved to be a valuable tool for gaining insight into challenges across the agency's infrastructure—not just limited to security. For example, when some video feeds from NDOT's traffic video network were not appearing, engineers initially attributed the problem to recently installed anti-virus software. Data collected by Splunk, however, revealed that the video was indeed flowing, but the problem was with the browser used to display the footage.

When NDOT's information security officer used Splunk to find that some malicious files sent via FTP were being written to a set of non-public folders, she used Splunk to uncover a faulty script. Upon fixing the problem, she then used Splunk to identify contractors and engineers who no longer use the FTP server and, for another safeguard, closed their accounts. Additionally, after staff had invested several weeks trying to determine why periodically some remote employees were unable to log into the network, insights from Splunk enabled staff to identify the issue and correct it within days.

For an unexpected benefit, NDOT has deployed Splunk to improve operational efficiencies. In one case, a large color printer/copier had become extremely costly to own because of its consumption of color inks. When discussions arose about replacing the device with an inkjet printer for each employee in the office, staff collected printing logs in Splunk. They found that the printer's default setting was color rather than black and white, causing excess use of the color cartridges. Resetting the printer turned out to be more cost-effective than replacing it with multiple inkjet printers, a discovery that has saved the department thousands of dollars. They even identified the printer's heaviest users to curtail their usage and further contain costs.

"Whenever there's a problem, we immediately go to Splunk for optics and intelligence," the ISO explains. "Splunk has empowered us to plug security gaps, improve efficiencies and save taxpayer money. We're limited only by our imaginations as to all the ways we can leverage the platform."

As with many Splunk deployments, NDOT has greatly expanded on its original use case for the platform. Going forward, NDOT plans to enhance public safety by funneling logs from the state's 511 system into Splunk to ensure information is always accurate and up-to-date. The staff will use Splunk to monitor the department's help desk system, Oracle databases, and more Active Directory logs, and plans to deploy the Google Maps for Splunk module on top of the Splunk platform to visually geo-locate data on maps of the state. Moreover, NDOT will determine the impacts of change policies and view the operation of devices over time to learn if any are approaching thresholds that may compromise their performance.

"As we increasingly rely on Splunk, we're traveling from being reactive to proactive," concludes NDOT's information security officer. "We're gaining the intelligence to know when a device or application will be overtaxed so we can take measures before problems arise, or when we can consolidate systems to stretch our budgets. Although Splunk has already demonstrated that it can help our agency improve public safety and operate more productively, efficiently and securely, we are just beginning to extract its full value."

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

Item # CS-Splunk-NDOT-101